Wireless Communications Policy

1.0 Purpose

This policy prohibits access to Kelvin TOP-SET Ltd networks via unsecured wireless communication mechanisms ("wireless networks"). Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Kelvin TOP-SET IT Staff are approved for connectivity to Kelvin TOP-SET Ltd networks. Usage of wireless networks will conform to the Company's Acceptable Usage Policy.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, mobile phones, tablets, etc.) connected to any of Kelvin TOP-SET Ltd internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and / or networks without any connectivity to Kelvin TOP-SET Ltd networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards

All wireless access points / base stations connected to the corporate network must be registered and approved by Kelvin TOP-SET IT Staff. These access points / base stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e. PC cards) used in corporate laptops, personal computers and workstations must be registered with the Kelvin TOP-SET IT Staff. The location of each access point must be registered with the Kelvin TOP-SET IT Staff. The installation of ad hoc wireless networks using desktop machines as access points is strictly forbidden.

3.2 Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations. Wireless networks must be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment. Kelvin TOP-SET IT may disconnect any wireless network that poses as security threat to the Company network or LAN.

3.3 Security

Wireless access points shall require appropriate user authentication before granting access to the corporate network or LAN. Physical security must be considered when planning the location of wireless access points. Wireless passwords and data must be encrypted. No application should rely on IP address-based security or reusable clear text passwords.

3.4 VPN Encryption and Authentication

All computers with wireless LAN devices must utilise the corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point-to-point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e. a MAC address.

3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the Company name, division, title, employee name, or product identifier. In some instances the SSID may be suppressed.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
A contractor found to have violated this policy would be liable to their contract to provide a service terminated.

5.0 Definitions

Term **Definitions**

Wireless Network A wireless network allows computers to share printers, files or an Internet connection without any wires between them. Wireless networking hardware uses radio frequencies to transmit information between the individual computers; each computer requires a wireless network adapter. A wireless network hub or router is used to bridge the wireless network to traditional networks, or provide a shared internet connection.

Access Point An access point is the connection that ties wireless communication devices into a network. Also known as a base station.

User Authentication A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

VPN A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures.

LAN A local area network (LAN) is a computer network covering a local area, like a home, office or small group of buildings.

SSID Service Set Identifier (“SSID”), is a sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network.

6.0 Revision History

Who	**Date**	**Revision Type**	**Revision Number**
Scott Bowden	20/10/2021	Initial draft	V0.1
Scott Bowden	14/03/2022	Updated	V0.2
Scott Bowden	30/01/2024	Annual check/update	V0.3